

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

MAY 27 2017

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT 370 HOLLAND LANE,
UNIT 3013, ALEXANDRIA, VA, 22314, MORE
PARTICULARLY DESCRIBED IN ATTACHMENT ACase No. 1:17-SW- (UNDER SEAL)
274

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized);

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
31 USC 5314, 5322	Failure to file Foreign Bank Account Reports
22 USC 618	Violation of Foreign Agent Registration Act
26 USC 7206(a)	Filing a False Tax Return

The application is based on these facts:

☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

[REDACTED]

Applicant's signature

Printed name and title

/s/

Sworn to before me and signed in my presence.

Date: 5/27/2017

City and state: Alexandria, VA

Theresa Carroll Buchanan
United States Magistrate Judge

Judge's signature

Hon. Theresa Carroll Buchanan, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAY 27 2017

IN THE MATTER OF THE SEARCH
OF THE STORAGE UNIT LOCATED AT
370 HOLLAND LANE, UNIT 3013,
ALEXANDRIA, VA, 22314,
MORE PARTICULARLY DESCRIBED
IN ATTACHMENT A

) Case No. 1:17-SW- 294

) (Under Seal)

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

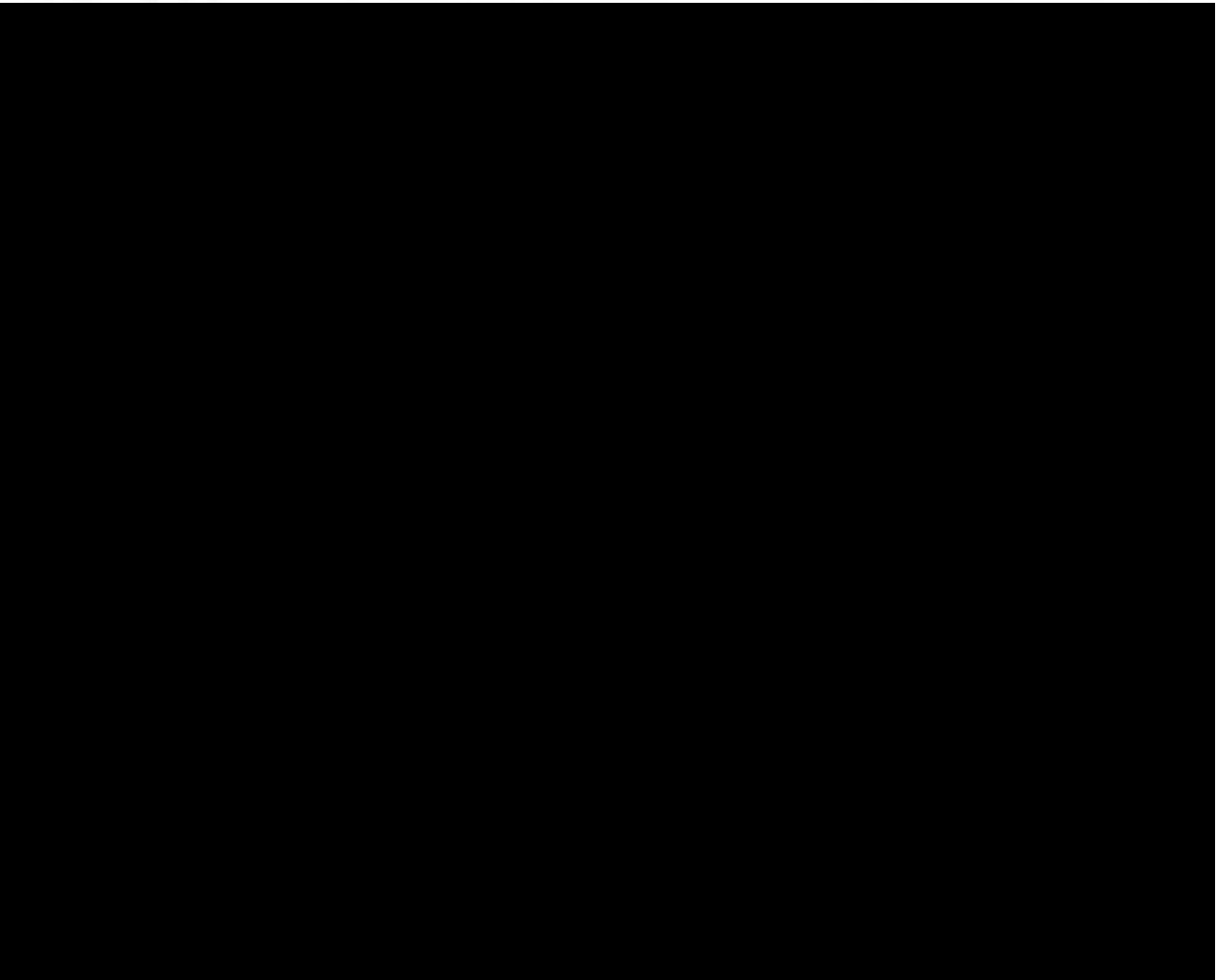
1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to search the storage unit located at 370 Holland Lane, Unit 3013, Alexandria, Virginia 22314, which is described more particularly in Attachment A, in order to locate and seize the items described in Attachment B. Both Attachment A and Attachment B are incorporated by reference as though fully set forth in this affidavit.

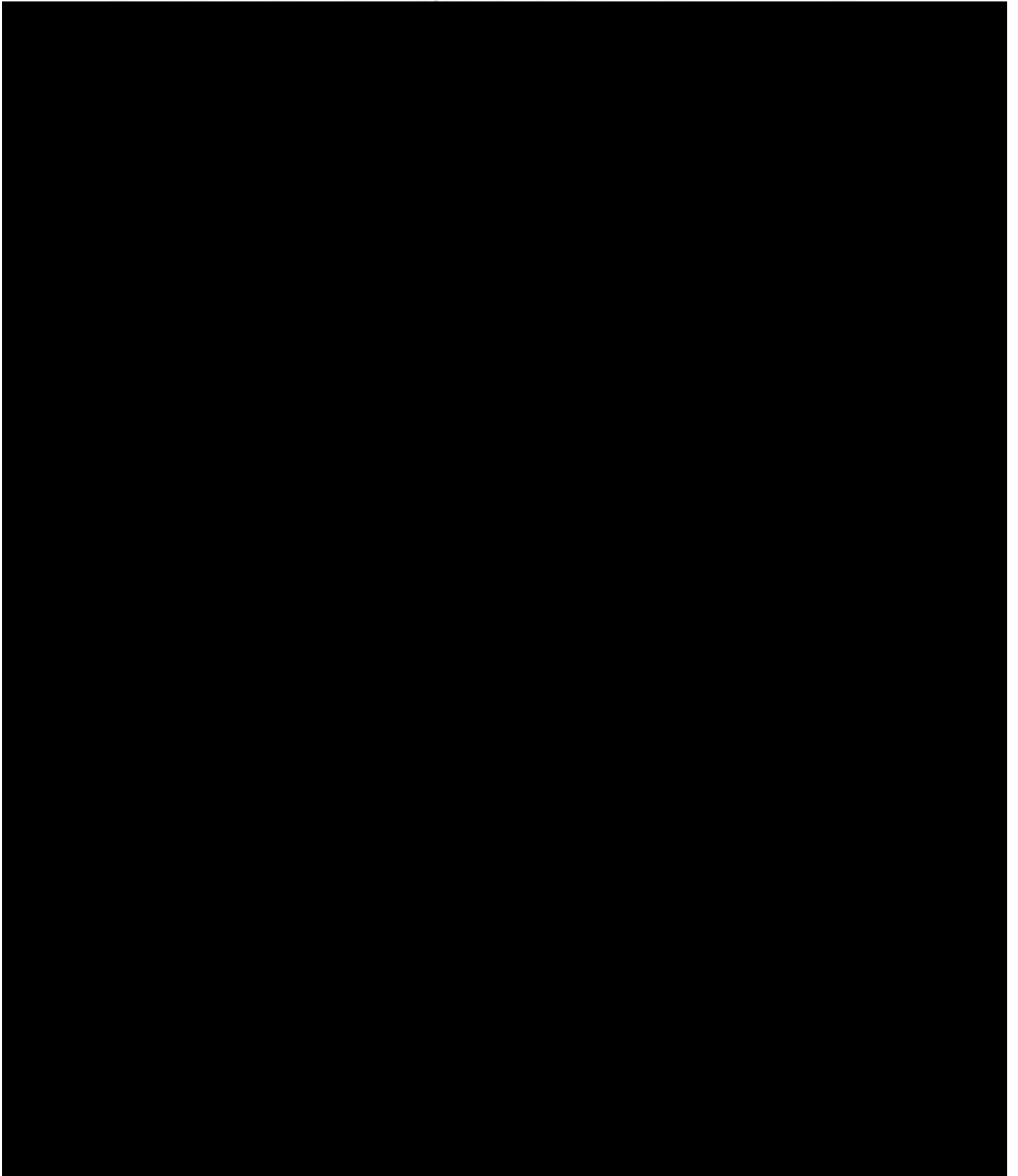
2. I have been a Special Agent with the FBI since 2002. I have received basic law enforcement training at the FBI Academy in Quantico, Virginia. I am currently assigned to the FBI's International Corruption Squad in Washington, DC, where I am responsible for conducting and assisting in investigations relating to international corruption, money laundering, violations of the Foreign Corrupt Practices Act, and other related financial crimes.

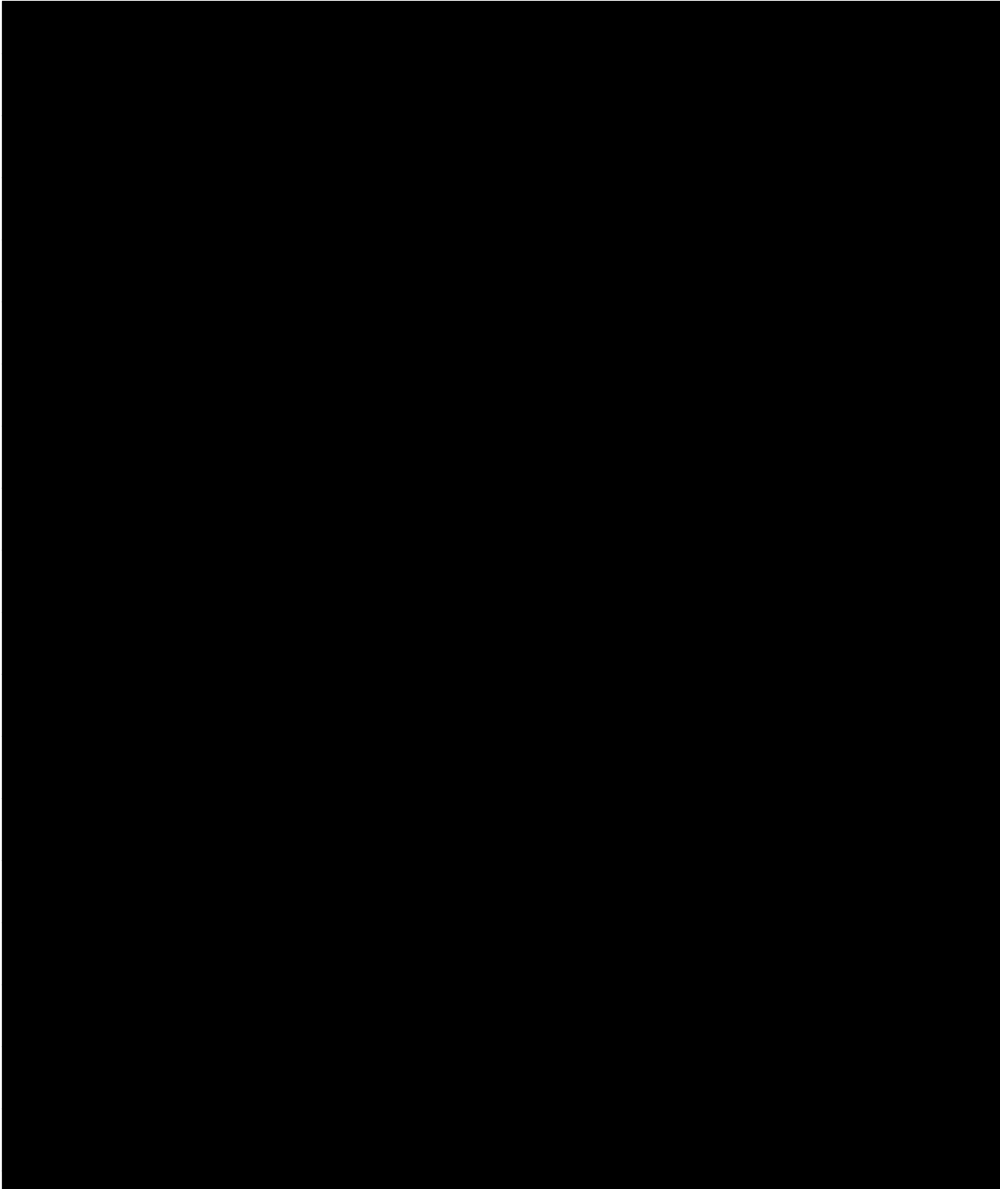
3. The facts in this affidavit come from my personal observations, my training and experience, a review of documentary evidence, information provided by witnesses, and information obtained from other law enforcement agents. This affidavit is intended to show

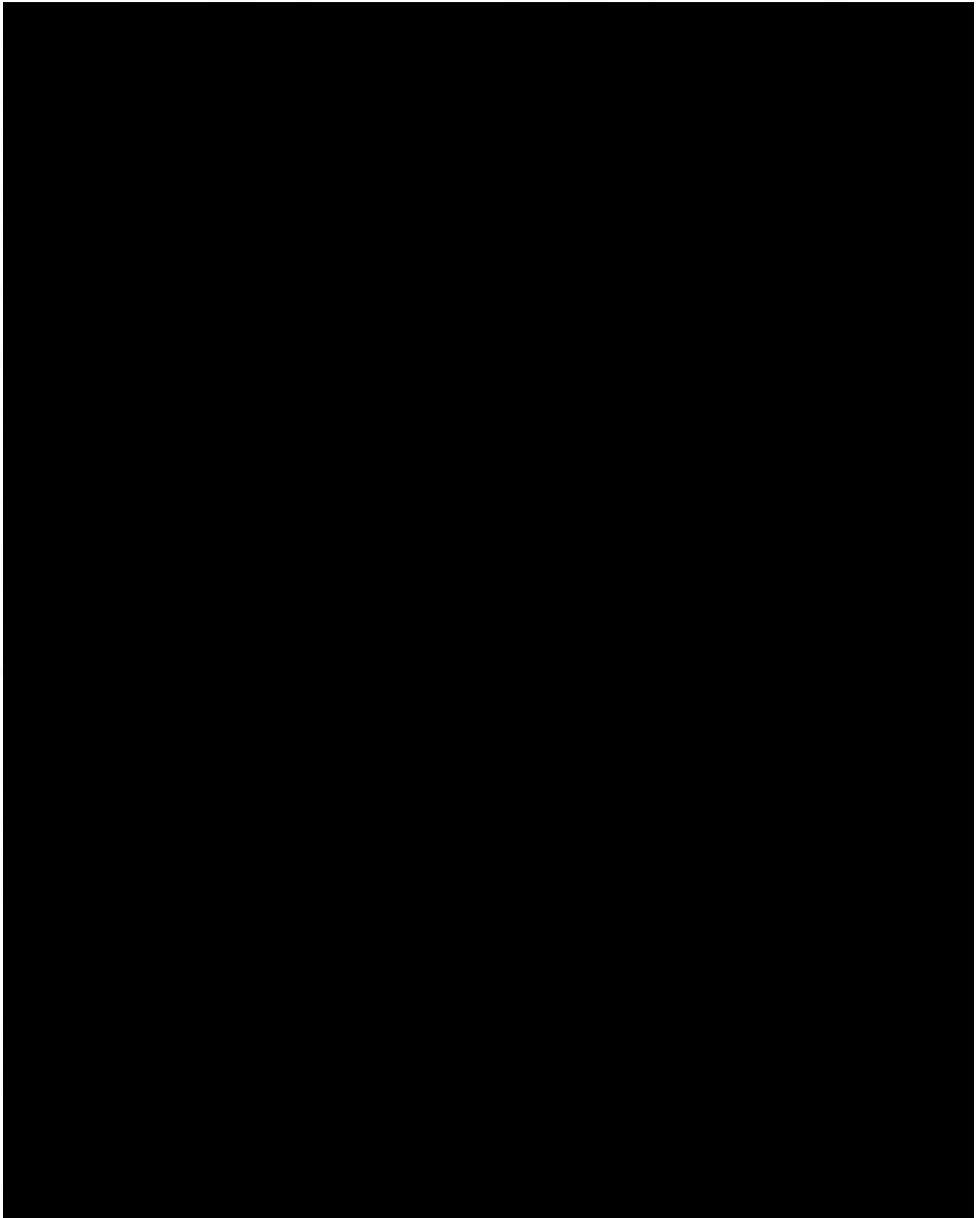
merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

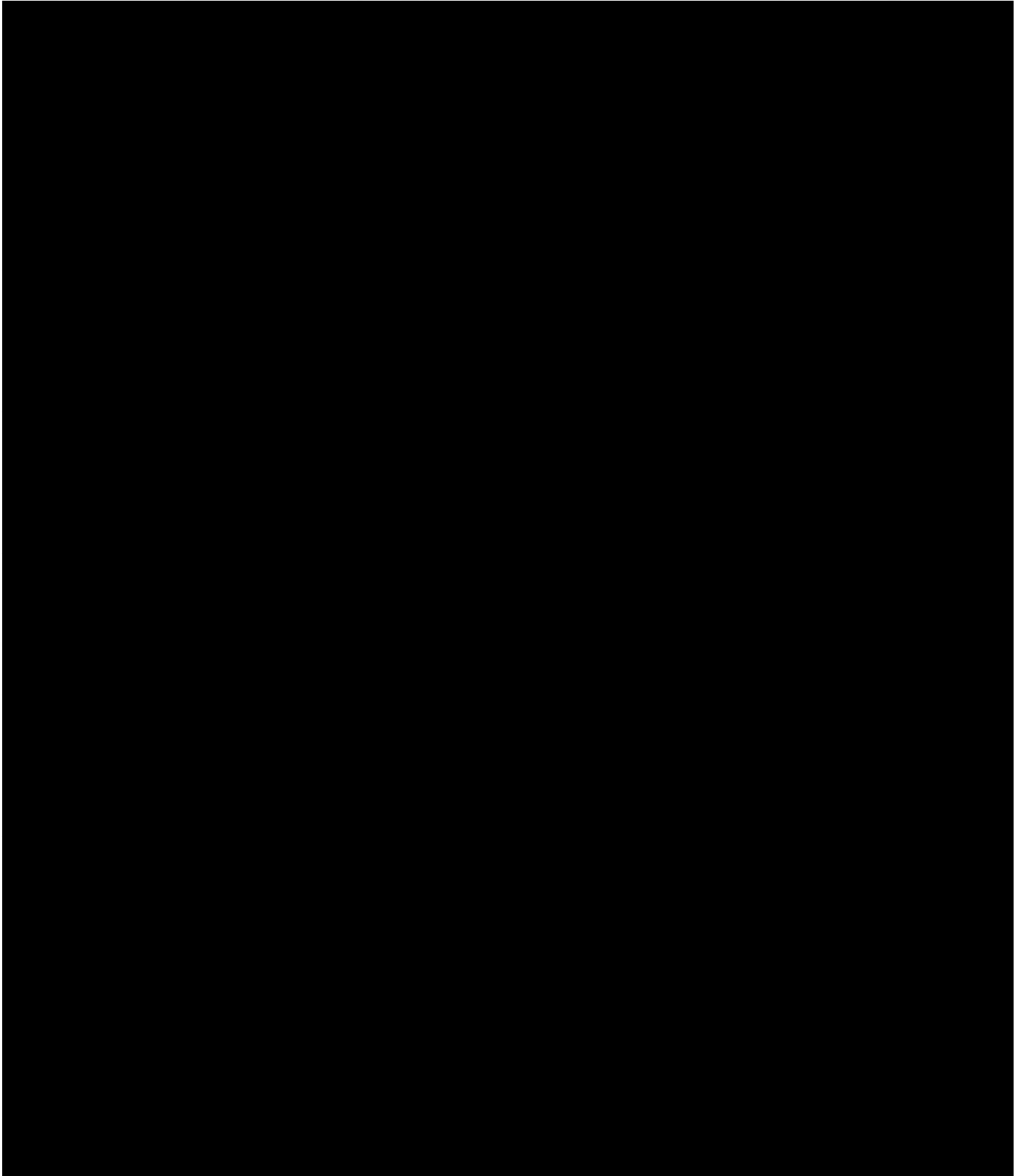
4. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of 31 U.S.C. §§ 5314, 5322(a) (Failure to File a Report of Foreign Bank and Financial Accounts), 22 U.S.C. § 618 (Foreign Agent Registration Act), and 26 U.S.C. § 7206(a) (Filing a False Tax Return), have been committed, and that there is probable cause to search the premises described in Attachment A for evidence, instrumentalities, contraband, or fruits of the crimes further described in Attachment B.

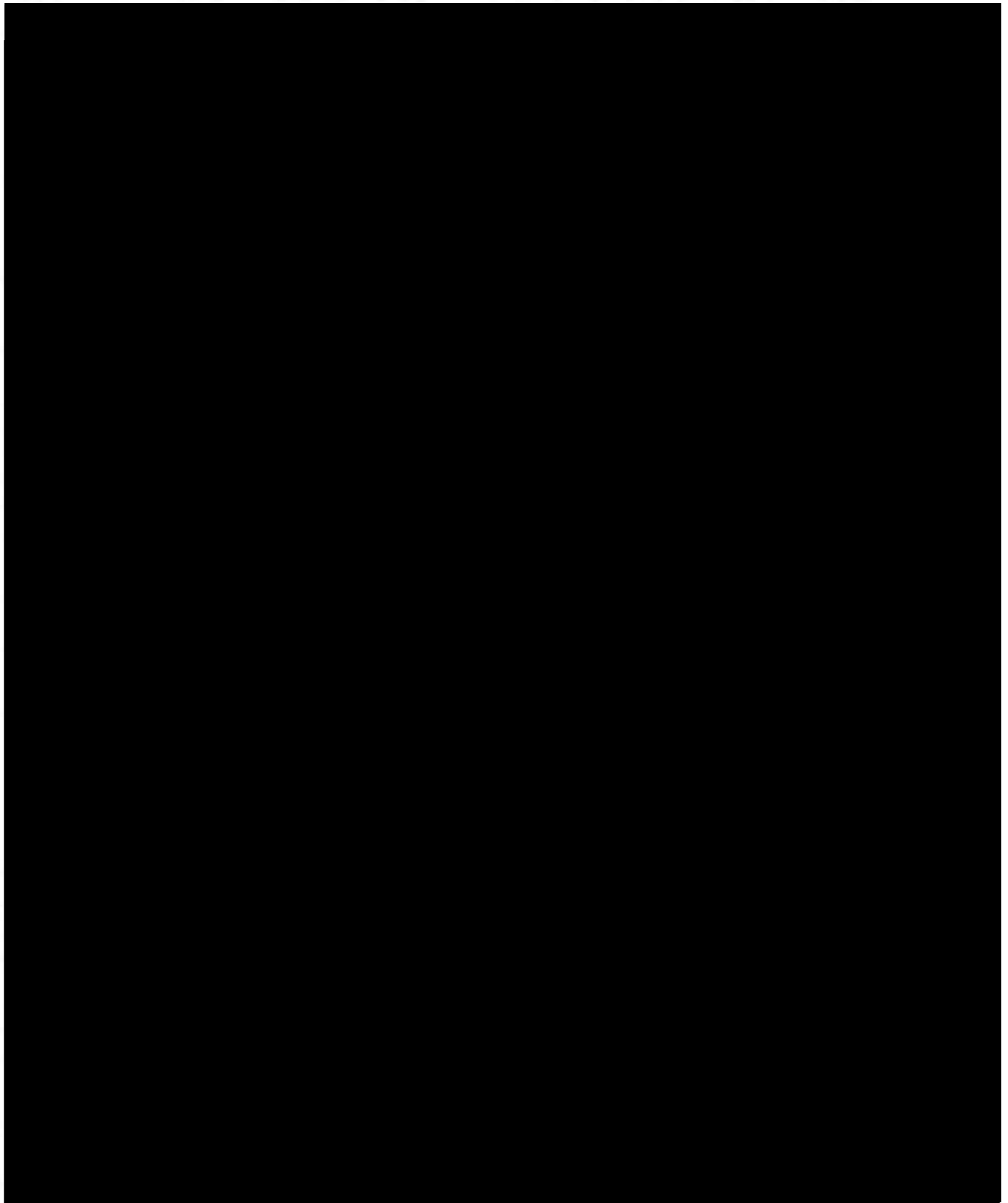


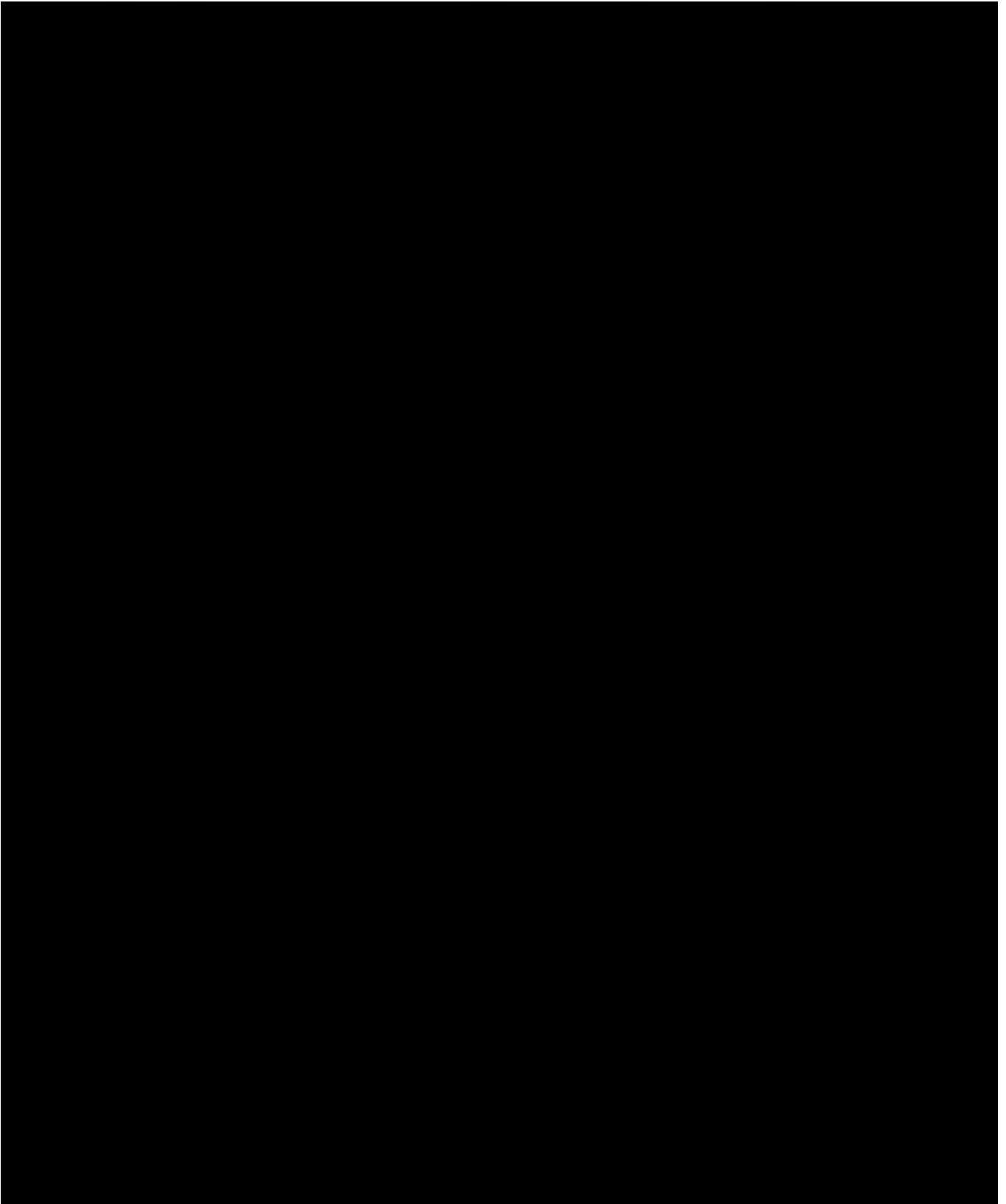


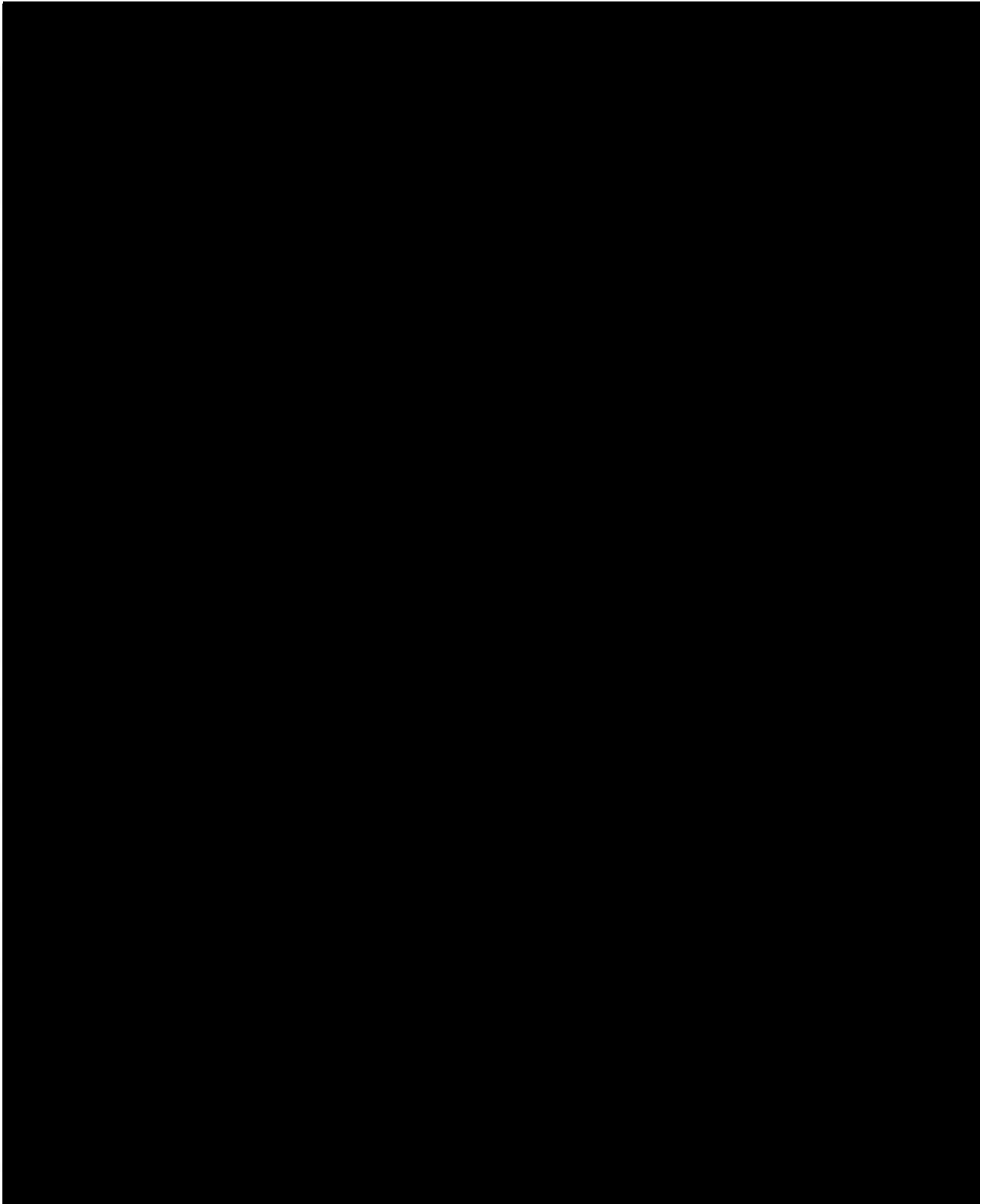












28. On May 26, 2017, your Affiant met with [REDACTED], a former employee of

Davis Manafort Partners, and a current employee of Steam Mountain, LLC, which is a business currently operated by Paul Manafort. [REDACTED] advised that he is a salaried employee of Manafort's company, and that he performs a variety of functions for Manafort and his companies as directed by Manafort. [REDACTED] advised that, in approximately 2015, at the direction of Manafort, [REDACTED] moved a series of office files of Manafort's business contained in boxes from one smaller storage unit at 370 Holland Lane, Alexandria, Virginia, to a larger storage unit, at the same storage facility, also at 370 Holland Lane, Alexandria, Virginia. [REDACTED] advised that he personally moved the office files into Unit 3013 at that location, and that the files were still in that unit.

29. Later on May 26, 2017, [REDACTED] led your Affiant to the storage facility at 370 Holland Lane, Alexandria, Virginia, where your Affiant obtained a copy of the lease for Unit 3013 from the manager of the storage facility. The lease identifies [REDACTED] as the occupant of Unit 3013, and also identifies Paul Manafort as a person with authorized access to Unit 3013. Richard Gates is listed as an alternate point of contact for the lease.

30. [REDACTED] further provided law enforcement with a key to the lock on Unit 3013 and described the contents of Unit 3013. [REDACTED] advised that Unit 3013 contained several boxes of office files from Manafort's business, as well as a metal filing cabinet containing additional, more recent office files of Manafort's business. [REDACTED] said he moved the filing cabinet from Manafort's former residence in Mount Vernon, Virginia, in the spring of 2015. [REDACTED] indicated that Manafort was using his former residence as an office at the time. [REDACTED] explained that the cabinet was extremely heavy when he moved it, indicating that it contained a large amount of records. Although [REDACTED] could not describe the contents of the filing cabinet in detail, he advised that Manafort occasionally sent emails to [REDACTED] directing [REDACTED] to put certain records

into the filing cabinet on Manafort's behalf. [REDACTED] described the records as "brown, legal-sized files." [REDACTED] recollection is that he last added to the filing cabinet in the spring of 2016.

31. Your Affiant obtained written consent from [REDACTED] to search Unit 3013. [REDACTED] then opened Unit 3013 using the key in his possession in the presence of your Affiant. Without opening any boxes or filing cabinet drawers, I observed inside the unit that there were approximately 21 bankers' boxes that could contain documents, as well as a five-drawer metal filing cabinet. None of the file drawers are marked as to their contents. Some of the boxes are unmarked, while others bear markings. For example, one of the bankers' boxes is marked on the exterior with the following:

Box 2

MPI

- Legal Docs
- Promissory Notes
- Admin
 - o Tax Returns
 - o BOD Resolution
 - o Written Consent of Sole Manager
 - o Seiden COI Waiver
 - o Resignation Letters
 - o Certificate of Liability Insurance
 - o Director's Insurance
 - o Trade Mark
 - o Worker's Comp
 - o MPI Holdings LLC
- Binder contains documents executed in connection with formation and financing of MPI Holdings LLC

32. Another box is marked on the exterior as follows:

Box 5

MPI

- Expenses
- Paid Bills
- Invoices
- Legal Complaints
- Jules Nasso

33. Your Affiant has determined from a search of a public records database that MPI stand for Manhattan Productions International, a film production company, for which Manafort is believed to be an investor. The name suggests that the company has an international scope. Accordingly, it is reasonable that these records may contain evidence of solicitations for and financial transactions involving foreign persons or sources of funds.

34. Another box is marked on the exterior as follows:

Box 12
Ukraine Binders
- Georgia
- Ballot Security
- Surrogates
- Admin
- Research
- RA
- Political
- Polling
- PJM Political Presentation
- Ukraine Campaign
- Media Earned
- Media
- Advance and Training
- Leader

35. For a number of reasons set forth herein it is reasonable to believe that this storage unit is a collection point for Manafort's and Gates's business records from their work in Ukraine. These include that there is a box marked "Ukraine," that [REDACTED] has advised the affiant that he moved business records for Manafort into the storage unit, and because Manafort and Gates—who is listed on the lease as a contact for the lessor—worked together in Ukraine. It is also reasonable to believe that these records and those in the filing cabinet will include financial records for several reasons. These include, but are not limited to, IRS guidelines recommending that persons and corporations generally retain business records for three years from filing of

returns for and seven years if the tax payer had certain losses or bad debts.

36. Your affiant also saw a box marked "movie production stuff," four boxes marked "'96 convention," and three boxes marked "1979 convention," "1988 convention" and "1992 convention, respectively. Because the records go back over 30 years, I believe records relating to Manafort's and Gates's work in Ukraine, including financial records, were retained and may be contained within the storage unit.

37. From my training and experience, I am also aware that individuals and businesses often retain copies of contracts and other business and financial records in anticipation of litigation. Public sources reveal that Manafort was sued by his former client, Oleg Deripaska, sometime in or about 2008. Therefore, it is reasonable to believe historical records have been retained by Manafort and Gates.

38. After I accompanied [REDACTED] to the storage unit described in Attachment A and conducted a review of the contents without opening any box or file drawer on May 26, 2017, the unit was locked with a key. Access to the facility by leaseholders and members of the public was foreclosed by the company from 9:00 pm on May 26, 2017 until approximately 7:00 am on May 27, 2017. Law enforcement agents have surveilled the only entrance and exit to the unit since the time the unit was locked on May 26, 2017 until 9:00 pm, and beginning again at 6:30 am on May 27, 2017, before the business was open to the public or leaseholders. No one has been observed entering or leaving the unit.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. In my training and experience, I have learned that U.S. businesses routinely generate and maintain records of correspondence and financial records on computers. For a variety of reasons, copies of historical records and current records are frequently stored on

external hard drives, thumb drives and magnetic disks. There is reasonable cause to believe such media may be contained in and among records of the Mananfort's and Gates's business in the storage unit.

40. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES described in Attachment A, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media.³ Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

³ A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

42. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the

search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under

investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
43. *Necessity of seizing or copying entire computers or storage media.* In most cases,

a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or

knowledge will be required to analyze the system and its data on the Premises.

However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

44. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.


REQUEST FOR SEALING

45. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, and many of the details of the investigation are not yet public. Accordingly, there is good cause to seal these documents because their premature disclosure may give subjects and witnesses an opportunity to move outside of U.S. jurisdiction or to destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation. Similarly, witnesses located abroad may take steps to compromise the investigation.


CONCLUSION

46. Based on the foregoing, I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,


[REDACTED]
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 5/27, 2017



/s/ Theresa Carroll Buchanan
United States Magistrate Judge
THERESA CARROLL BUCHANAN
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched is the storage unit located at 370 Holland Lane, Unit 3013, Alexandria, Virginia 22314, as well as any locked drawers, locked containers, safes, computers, electronic devices, and storage media (such as hard disks or other media that can store data), found therein. The storage unit is further described as a metal corrugated steel room with a red and white sign on the exterior with the number 3013.

ATTACHMENT B

Property to be seized

1. Records relating to violations of 31 U.S.C. §§ 5314, 5322(a) (Failure to File a Report of Foreign Bank and Financial Accounts), 22 U.S.C. § 618 (Foreign Agent Registration Act), and 26 U.S.C. § 7206(a) (Filing a False Tax Return), including:

- a. Any and all financial records for Paul Manafort, Richard Gates or companies associated with Paul Manafort or Richard Gates, including but not limited to records relating to any foreign financial accounts;
- b. Any and all federal and state tax documentation, including but not limited to personal and business tax returns and all associated schedules for Paul Manafort, Richard Gates, or companies associated with Paul Manafort or Richard Gates;
- b. Letters, correspondence, emails, or other forms of communications with any foreign financial institution, or any individual acting as the signatory or controlling any foreign bank account;
- c. Any and all correspondence, communication, memorandum, or record of any kind relating to the Party of Regions, Viktor Yanukovich, the European Centre for a Modern Ukraine, or any other foreign principal of Paul Manafort or Richard Gates, or any company associated with Paul Manafort or Richard Gates;
- d. Any and all correspondence, memorandum, press release, or documentation of any kind regarding any lobbying or advocacy performed by Paul Manafort, Richard Gates, or any company associated with Paul Manafort or Richard Gates, on behalf of the Party of Regions, Viktor Yanukovich, the European Centre for a Modern

Ukraine, or any other foreign principal of Paul Manafort, Richard Gates, or any company associated with Paul Manafort or Richard Gates.

- e. Records related to, discussing, or documenting Neocom Systems, Antes Management, Yiakora Ventures, Global Highway Ltd., Global Endeavor, Leviathan Advisors, Peranova Holdings, Bletilla Ventures, Lucicle Consultants, and/or Telmar Investments, including but not limited to bank records, canceled checks, money drafts, letters of credit, cashier's checks, safe deposit records, checkbooks, and check stubs, duplicates and copies of checks, deposit items, savings passbooks, wire transfer records, and similar bank and financial account records.
 - f. Records related to, discussing, or documenting the Podesta Group.
 - g. Any and all daily planners, logs, calendars, schedule books relating to Paul Manafort or Richard Gates.
- 2. Computers or storage media used as a means to commit the Target Offenses.
 - 3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web

pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.